

THE CATHOLIC UNIVERSITY OF AMERICA
COLUMBUS SCHOOL OF LAW

Legal Studies Series

Accepted Paper No. 2022-2 Date: 2022



§230 of the Communications Decency Act: Regarding Child Sexual Abuse Material - The Experiment is Done and it Failed

Mary Graw Leary

40 Cardizi Arts & Ent. L.J. _ (forthcoming 2022).

This paper can be downloaded without charge from
the *Social Science Research Network* electronic library at:

<http://ssrn.com/abstract=4254010>

Legal Studies Series Editor – Elizabeth Edinger: edinger@law.cua.edu

The Columbus School of Law – <http://law.cua.edu/>



§230 of the Communications Decency Act: Regarding Child Sexual Abuse Material - The Experiment is Done and it Failed

Mary Graw Leary

The Catholic University of America

Special thanks to the staff of the Cardozo Journal for Law and Entertainment for their patience. I am deeply grateful to Katie Jung and Mariyah Wakhariya for outstanding research; to Steve Young for unfailing library and research support; to Jeff Kosseff, Sarah Duggin, and Yiota Souras for their insight; to the faculty of the Catholic University of America Law School for their comments, and to the brave victim survivors of child sexual abuse material who share their experiences, so others can be protected.

Draft - Not For
Circulation

Twenty years ago, these online images were a problem;

10 years ago, an epidemic.

Now, the crisis is at the breaking point.¹

Introduction

In 1996 Bill Clinton was President, “Macarena” topped the Billboard charts, and The English Patient won the Oscar for best picture. Netscape Navigator was the most popular web browser, Jerry’s Guide to the World Wide Web had recently changed its name to Yahoo!, and Google.com did not exist.² The average American with Internet access spent fewer than 30 minutes a month “surfing the web” through their dial up connection.³ It was also the year that Congress attempted to update the 62 year old Communications Act of 1934 to adapt to the then modern world of cable television over telephone lines, the new “information superhighway,” and a more modern role for the Federal Communication Commission. The Telecommunication Act of 1996 endeavored to achieve these goals with a targeted lifespan of 10 – 15 years, when some legislators predicted they would have to update the law again.⁴

Within this massive bill was a now famous component referred to in modern parlance as “Section 230 (§230).” Section 230 is a component of the Communications Decency Act which itself is a component of the Telecommunications of Act of 1996. A statute that has been

¹ Michael H. Keller and Gabriel J.X. Dance, *The Internet is Overrun with Images of Child Sexual Abuse. What Went Wrong?*, N. Y. TIMES (Sept. 29, 2019), <https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html>.

² Tech Musings, *The Web Back in 1996-1997*, SOLARWINDS PINGDOM (Sept. 16, 2008), <https://www.pingdom.com/blog/the-web-in-1996-1997/>.

³ Farhad Manjoo, *Jurassic Web*, SLATE (Feb. 24, 2009), <https://slate.com/technology/2009/02/the-unrecognizable-internet-of-1996.html>.

⁴ TELECOM-LH 109, 1996 WL 33665756 (A.&P.L.H.), 1 (“I predict that this will be succeeded someday as we get into the wireless age by another act, maybe in 10 or 15 years. But this Telecommunications Act will provide us with a road map into the wireless age and into the next century.”); *see also* Stuart N. Brotman, *Was The 1996 Telecommunications Act Successful in Promoting Competition?*, BROOKINGS (Feb. 8, 2016), <https://www.brookings.edu/blog/techtank/2016/02/08/was-the-1996-telecommunications-act-successful-in-promoting-competition/> (The goal of the 1996 Telecommunications Act was to “set a framework based on those enduring principles of competition and open entry, allow a little time for the industry to get used to the ideas, and get out of the way.”).

expanded far beyond its original purpose, some attribute the scope of the Internet today directly to the passage of §230. Others point to §230 as the statute responsible for many of the problems present across the Internet.

Decades later, whether the current state of the Internet is positive or negative often depends upon one's perspective. Much of the tech industry, their surrogates, and proponents of an unregulated Internet argue that §230 should be celebrated for creating a thriving Internet. Critics point to the broad immunity §230 has come to represent, which shields many Internet platforms from liability for harms caused by an Internet with no oversight but incentives for boundless profit. They argue it is time to revisit its provisions and adapt them for the modern era.

Nowhere is this debate occurring more vigorously than in the area of child protection. Two truths are evident. The Internet has brought with it tremendous opportunities for learning, connection, and business. Also not in dispute is the fact that the Internet and other digital platforms have led to an unprecedented exploitation of children on a scale never before seen. Recognizing these two realities, a debate thrives about the proper role of §230 in the modern world - a world very different from 1996. In the last two Congressional terms, representatives and senators filed dozens of bills to amend or repeal §230,⁵ a President issued an Executive Order⁶ regarding its effect on political speech, and the Department of Justice launched a series of

⁵Meghan Anand et al., *All The Ways Congress Wants To Change Section 230*, SLATE (Mar. 21, 2021), <https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html>.

⁶Executive Order 13925, Preventing Online Censorship, 85 Fed. Reg. 106 at 34079 (May 28, 2020); Anshu Siripurapu, *Trump and Section 230: What to Know*, COUNCIL ON FOREIGN REL. (Dec. 2, 2020), <https://www.cfr.org/in-brief/trump-and-section-230-what-know>.

recommendations on reforming the Section.⁷ In these debates, the sides emphasize, *inter alia*, what §230 was intended to do as if that solely determines its social utility today.

This article focuses on the issues surrounding child exploitation. It does so because, some in the modern debate attempt to reframe §230's origin as one singularly focused on Internet freedom. What is often missed in the discussion of §230 is the actual context in which it became law. That context was partially as a piece of legislation emerging from within a landscape of child protection.⁸ That is not to say it is limited to being a child protection statute and this article does not assert such a position. Section 230 is not solely concerned with child protection. However, it emerged from a larger discussion of the most effective ways to limit explicit material online and protect children. Therefore, unlike the many other issues that spark §230 debate – political speech, e-commerce, misinformation, antitrust issues – the child protection issues are more easily assessed when one is reminded that §230 was, in part, an effort to address child protection on the Internet. Once restored to this original context, the efforts to reform §230 seem more clear and more critically needed in the present day.

This article revisits the history of §230, its connection to child protection, and corrects the artificial reframing of §230 as legislation focused only on an unregulated Internet. It examines the child protective landscape from which it emerged and the promises its proponents made regarding protection. It then compares those intentions and promises to the present day climate regarding child exploitation on the Internet, specifically focusing on the problem of Child Sexual

⁷ *Department of Justice's Review of Section 230 of the Communication Decency Act Of 1996*, DEP'T. OF JUST. ARCHIVES, <https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996>.

⁸ As will be discussed, legislators addressed concerns regarding the exposure of children to explicit images which includes child sexual abuse material, as well as other aspects related to such materials; *e.g.*, 142 Cong. Rec. 1993, 2030 (comments of Sen. Coats) (discussing images dealing with the sexual abuse of children).

Abuse Material (CSAM) – also known as child pornography in the United States.⁹ Observing the cavernous fissure between one of the many intentions of §230 and the reality of online child exploitation it argues that the need to reform §230 is now and return §230 to one of its original purposes. This article argues that need is prescient not only because of the grave reality of CSAM online, but also because of one of the very intentions behind §230. By updating §230 at least in the area of CSAM, §230 will be returned to one of its original intents to assist in child protection or at least no to longer be a facilitator of child sexual exploitation.¹⁰

I. § 230's History Demonstrates It Should Be Understood as a Component of a Larger Child Protection Landscape

In 1995 and 1996 Congress took on a daunting task – a task with which they had been struggling for years – updating the national telecommunications law. By the late 1990's, the Communications Act of 1934 had long outlived its utility. With cable television, digital communication, and the growing advent of the Internet, Congress understood it must adjust its regulatory framework. Congress also recognized that among the many benefits of the nascent Internet were some potential serious social costs. One of these costs was a proliferation of sexually explicit material – some of which was violent, obscene, or involving children – on the

⁹E.g., Terminology and Semantics: Interagency Working Group on Sexual Exploitation of Children, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, (ECPAT Int'l. pub., Lux., Jan. 28, 2016) (While “child pornography” is the term originally used for images of children subject to sexual abuse and exploitation, globally, the preferred term is CSAM. The word “pornography” often depicts adults in often consensual sexual acts. CSAM consists of photographs and video footage of child sexual abuse and the term “child sexual abuse material” more accurately reflects its illegal and unprotected content).

¹⁰ A word must be said about the actual content of CSAM. Such images are not merely sexually suggestive and efforts to sanitize their graphic nature should be rejected. Rather, they are images of children engaged in sexually explicit conduct which, under federal law includes “actual or simulated—

- (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
- (ii) bestiality;
- (iii) masturbation;
- (iv) sadistic or masochistic abuse; or
- (v) lascivious exhibition of the anus, genitals, or pubic area of any person.”

18 U.S.C. 2256(1)(A). As will be discussed supra these images are often of very young children and increasingly more severe.

Internet. Section 230 emerged as part of the solution to preclude the spread of that material online.

In advocating for section 230 to be interpreted broadly, tech companies and their surrogates have successfully skewed the purpose of the legislation. They suggest it was created as a stand alone piece of legislation to create a robust Internet free of government regulation of almost any kind and designed almost exclusively as a haven for all speech.¹¹ “Whenever there is discussion of repealing or modifying the statute, its defenders, including many technology companies, argue that *any alteration* could cripple online discussion.”¹² For example, the Electronic Frontier Foundation labels Section 230 as “the most important law protecting internet speech.”¹³ A commentator states that Congress’ purpose was to “reduce the risk that platforms will quash free speech due to fears of lawsuits...”¹⁴ and another argued that “Congress was concerned that tort based lawsuits could chill speech and innovation.”¹⁵ Such advocacy has lost focus on the context of section 230. Consequently, “[c]ourts have construed the immunity provision in Section 230 broadly in all cases arising from the publication of ‘user generated’ content.”¹⁶

¹¹ See Daisuke Wakabayashi, *Legal Shield for Social Media Targeted By Lawmakers*, N. Y. TIMES (May 28, 2020), <https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html> (describing the “full throated” defense of Section 230 by Google, Facebook, and Twitter executives.).

¹² Daisuke Wakabayashi, *Legal Shield for Social Media Targeted By Lawmakers*, N. Y. TIMES (May 28, 2020), <https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html>.

¹³ *CDA 230: The Most Important Law Protecting Internet Speech*, EFF, <https://www.eff.org/issues/cda230>; see also Casey Newton, *Everything you Need to Know about Section 230*, VERGE (Dec. 29, 2020), <https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation> (describing Section 230 as “the most important law for online speech”).

¹⁴ Derek Bombauer, *How Section 230 Reform Endangers Internet Free Speech*, BROOKINGS (July 1, 2020), <https://www.brookings.edu/techstream/how-section-230-reform-endangers-internet-free-speech/>; see Daisuke Wakabayashi, *Legal Shield for Social Media Targeted By Lawmakers*, N. Y. TIMES (May 28, 2020), <https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html> (“Section 230 has allowed the modern internet to flourish.”).

¹⁵ Farnaz Alemi, *Section 230 Under Assault: Not Just a Big Tech Problem*, JDSUPRA (Apr. 14, 2021), <https://www.jdsupra.com/legalnews/section-230-under-assault-it-s-not-just-1029515/>.

¹⁶ *Doe v. Myspace, Inc.*, 528 F.3d 413, 418 (2008); Section 230 — Nurturing Innovation or Fostering Unaccountability?, U.S. Dep’t of Just. (“[C]ourts have interpreted the scope of Section 230 immunity very broadly, diverging from its original purpose.”).

A. History of the Communications Decency Act in the Senate

One effort to address the feared expansion of sexually explicit material on the Internet was The Communications Decency Act (CDA), first introduced in the Senate in February of 1995.¹⁷ This bill addressed many aspects of communications including obscene or harassing use of telecommunication facilities, obscene programming on cable television and radio, increased penalties for violations, scrambling of explicit cable television channels for non-subscribers, etc.¹⁸ In June of 1995 its sponsor submitted a revised CDA as an amendment to the Telecommunications Act of 1995. This revised version again addressed several different issues regarding obscenity, computer harassment, and sexually explicit material.¹⁹ It extended “the anti-harassment, indecency, and anti-obscenity restrictions [then currently] placed on telephone calls to ‘telecommunication devices’ and ‘interactive computer services.’”²⁰ Among its provisions, it made it illegal to knowingly send or display in any manner available to a minor “any comment, request, suggestion, proposal, image or other communications that, in context, depicts or describes in terms patently offensive as measured by contemporaneous community standards sexual or excretory activities or organs, regardless of whether the user of such a service placed the call or initiated the communication.”²¹ In

¹⁷Robert Cannon, *The Legislative History of Senator Exon’s Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L. J. 51 (1996); 141 CONG. REC. 3203; *Force v. Facebook*, 934 F.3d 53 (2d. Cir. 2019).

¹⁸ The Communications Decency Act of 1995, S. 314, 104th Cong. (1995).

¹⁹Senator Exon, Letter to the Editor, WASH. POST, Dec. 2, 1995, at A20 (“[The Internet]” is a great boon to mankind. But we should not ignore the dark roads of porn [sic], indecency, and obscenity it makes possible.”).

²⁰Robert Cannon, *The Legislative History of Senator Exon’s Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L. J. 51 (1996); 141 CONG. REC. 3203; *Force v. Facebook*, 934 F.3d 53 (2d. Cir. 2019); 47 U.S.C. § 230(f)(2) (“The term “interactive computer service” (ICS) means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.”).

²¹47 U.S.C. § 223(a); Communications Decency Act of 1995 § 502.

other words, the CDA sought to hold ICS's potentially responsible for facilitating the spread of such images on their platforms. This revised version contained several defenses including the defense that the platform provided "mere access" to the material; respondent superior; a recognition of good faith attempts to comply with the statute; and protection against criminal or civil liability for making a good faith effort to restrict access to such material.²²

This legislation, although possessing many provisions, focused in part on child protection. "The fundamental purpose of the Communications Decency Act is to provide much needed protection for children."²³ It intended to not only to shield children from explicit content but to also prevent children from exploitative interactions or introductions with adult offenders.²⁴ The Report of the Senate Committee on Commerce, Science and Transportation also reflected these priorities. With regard to the CDA the committee expressed concern that the information highway "be safe for families and children" as well as concerns regarding channels being used to "transmit pornography, engage children in inappropriate adult contact, terrorize computer network users through 'electronic stalking,' and seize personal information."²⁵

In June of 1995, the child protection qualities of the proposed bill were debated, but proponents and opponents alike understood the focus to include explicit content and child protection. One of the bill's sponsors noted that the CDA "stands for the simple proposition: that is, the laws which already apply to obscene indecent, and harassing telephone use of the mail should apply to computer communications. That is the heart and soul of our amendment."²⁶

²² 47 U.S.C. § 223(c); Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L. J. 51, 59 (1996).

²³ 141 CONG. REC. S8088 (daily ed. June 9, 1997) (comments of Sen. Exon); *see also* 141 CONG. REC. S8089 ("The heart and soul of the Communications Decency act are its protections for families and children.").

²⁴ 141 CONG. REC. S1954 (daily ed. June 9, 1995) (comments of Sen. Exon).

²⁵ COMM. ON COM., SCI., AND TRANSP., THE TELECOMM. AND DEREGULATION ACT OF 1995, S. RPT. NO. 104-23, at 59 (1995).

²⁶ 141 CONG. REC. S8329 (daily ed. June 14, 1995) (comments of Sen. Exon).

Another supporter discussed the bill in terms of “one of our most important values is the protection of our children....”²⁷ The Senate debate was quite clear to include not only pornography but “the most hardcore perverse types of pornography, photos, and stories featuring child abuse and bestiality.”²⁸ Rather prophetically, Senators noted the need to protect children from child abuse itself on the Internet, endorsing the CDA as an effort to address “images and text that deal with sexual abuse of children... [and] infants.”²⁹

Although the provision passed through the Senate overwhelmingly 81-18, there were some opponents, but those opponents understood the purpose of Act, but opposed it for other reasons. They, recognized the Communications Decency Act as inherently a measure involving child protection. Senator Leahy recognized and shared the goal of the Act to “keep hardcore pornography away from our children,” but simply felt there was a less restrictive way to do so.³⁰ Another opponent applauded the sponsors’ focus on “the need to protect our children from obscene and indecent material.”³¹ Even then Senator Biden who opposed the Bill on First Amendment grounds described its “mission” as one of protecting children.³² In June of 1995, the Senate attached the CDA to the Senate version of the Telecommunications Act of 1995 as a clear child protective measure.

²⁷141 CONG. REC. S8332 (daily ed. June 14, 1995) (comments of Sen. Coats).

²⁸141 CONG. REC. S8330 (daily ed. June 14, 1995).

²⁹141 CONG. REC. S8332 (daily ed. June 14, 1995) (comments of Sen. Coats); *see also*, 141 CONG. REC. S8330 (daily ed. June 14, 1995) (Arguing support for the CDA as an amendment to the Telecommunications Act was an effort to side with “children threatened by abuse.”).

³⁰141 CONG. REC. S8331 (daily ed. June 14, 1995) (comments of Sen. Leahy) (Senator Leahy also wanted to limit government regulation); 141 CONG. REC. 16007 (“Child pornographers in my mind ought to be in prison. The longer the better. I am trying to protect the Internet and make sure that when we finally have something that really works in this country we do not step in and screw it up as sometimes happens with government regulation.”).

³¹141 CONG. REC. S8334 (daily ed. June 14, 1995) (comments of Sen. Feingold); *see also*, 141 CONG. REC. S8334, 8337 (“We share the goal of this provision but disagree as to the means to achieve that end.”).

³²141 CONG. REC. S8345 (daily ed. June 14, 1995) (comments of Sen. Biden).

B. History of the Internet Freedom and Family Empowerment Act In the House

In the House of Representatives, two Congressmen approached this issue differently than the Senate and Congressmen Christopher Cox and Ron Wyden introduced the Internet Freedom and Family Empowerment Act of 1995 (IFFE) as an amendment to the Telecommunications Act.³³ The IFFE addressed a wider breadth of issues, but still can be characterized as emerging from a child protection landscape, as it was in response to the original CDA. To be sure, IFFE sought to limit government regulation of the Internet.³⁴ But it also explicitly discussed this within the context of child protection. Indeed, Representative Cox, who later left Congress to become legal counsel and lobbyist on behalf of an association of online business and then a board member of said organization,³⁵ asserted that it was “designed as an alternative to the Exon approach.”³⁶ This approach distinguished between the content providers and those who provided access to the content. He argued for a framework in which interactive computer services (ICS)³⁷ were not

³³Internet Freedom and Family Empowerment Act, H.R. 1978, 104th Cong. (1995); *H.R.1978 – Internet Freedom and Family Empowerment Act*, CONGRESS.GOV (1995-1996), <https://www.congress.gov/bill/104th-congress/house-bill/1978>.

³⁴Robert Cannon, *The Legislative History of Senator Exon’s Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L. J. 51, 67 (1996) (citing 141 CONG. H8478-79 (daily ed. August 4, 1995) (Comments Rep. Cox)).

³⁵*Online Sex Trafficking and the Communications Decency Act, Testimony on Behalf of NetChoice before the U.S. House Committee of the Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations*, (2017) (statement of Christopher Cox, NetChoice), available at <https://netchoice.org/wp-content/uploads/2017-10-03-Testimony-of-Chris-Cox-on-behalf-of-NetChoice-before-House-Judiciary-Subcommittee-on-Crime.pdf>; *see also About Us*, NETCHOICE, <https://netchoice.org/about/> (listing its association members and founding as a “coalition for online businesses”); *Our Team*, NETCHOICE, <https://netchoice.org/team/chris-cox/> (listing Christopher Cox as Board Member).

³⁶Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, UNIV. RICH. J. L. AND TECH., 64 (2020); Rather perplexingly, Cox rejects the “myth” that his amendment was an amendment to the CDA, but also argues it was an alternative to it. As will be discussed *infra* the Conference Committee did not see it that way and combined the IFFE concepts to the CDA and both houses of Congress passed this component of IFFE as an amendment to the CDA.

³⁷ An “interactive computer service” is defined as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.” 47 U.S.C. 230(f)(2).

treated as publishers or as providers of the sexually explicit content. Although he did acknowledge that the ICS could also be content providers if they contributed to the content.³⁸

The IFFE was largely in response to a defamation case, *Stratton Oakmont, Inc. v. Prodigy Services Co.*³⁹ Prodigy operated a financial services bulletin board where members could post information about the world of finance. In so doing, Prodigy made an effort to monitor the board and edit out inappropriate comments. An anonymous post accused Stratton Oakmont of questionable dealings and Stratton Oakmont sued Prodigy for libel. In contrast to precedent, this state court agreed with Stratton Oakmont and found Prodigy responsible for that third party content in part because of its active role in screening out from the board any material it found inappropriate.⁴⁰ The court labeled it a publisher of the information under state law because “it voluntarily deleted some messages . . . and was therefore legally responsible for the content of defamatory messages that it failed to delete.”⁴¹ Perplexingly, this state court held a company responsible for third party content because that company made good faith efforts to remove inappropriate third party material from its platform, but would not have found it responsible if it had done nothing.⁴²

³⁸Robert Cannon, *The Legislative History of Senator Exon’s Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L. J. 51, 58 (1996).

³⁹No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. 1995), *superseded by statute*, Communications Decency Act of 1996, 47 U.S.C. § 230, *as recognized in* *Shiamilli v. Real Est. Grp. of New York, Inc.*, 952 N.E.2d 1011 (N.Y. 2011).

⁴⁰No. 31063/94, 1995 WL 323710, *2 (N.Y. Sup. Ct. 1995); *contra*, *Cubby, Inc. v. Compuserve, Inc.*, 776 F.Supp. 135 (SDNY) (Dismissing defamation action against defendant who sold access to library of news publications because defendant was a mere distributor and not a publisher.)

⁴¹Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008) (citing *Stratton Oakmont v. Prodigy Servs. Co.*, 1995 WL 323710, *4 (Sup. Ct. May 24, 1995)).

⁴²*Stratton Oakmont v. Prodigy Servs. Co.*, 1995 WL 323710 (Sup. Ct. May 24, 1995); *see also* *Doe v. AOL*, 783 So. 2d 1010, 104 (2001) (citing Steven M. Cordero, Comment, *Domnum Absque Injuria*, *Zeran v. AOL: Cyberspace Defamation Law*, 9 FORDHAM INTELL. PROP., MEDIA AND ENT. L.J. 775 (1999)).

IFFE, therefore, reflected a concern that courts could hold a platform responsible for content it did not create and disincentivize the company from monitoring its platforms. “[T]he statute’s fundamental principle is that content creators should be liable for any illegal content they create. Internet platforms are generally protected from liability for third party content, unless they are complicit in the development of illegal content, in which case the statute offers them no protection.”⁴³ However, child protection remained a backdrop of the discussion.

C. Amending the CDA with IFFE in Conference to Produce §230 in the Final Version of the CDA and Telecommunications Act of 1996

With these events, 1995 concluded with two different versions of the Telecommunications Act in each house of Congress. The bills went into conference where both houses negotiated a final bill. The CDA, while recognizing the value of the Internet,⁴⁴ sought to protect children and families from explicit content and to be an obstacle to child abuse and exploitation. The IFFE, while acknowledging the concerns of the CDA, wanted to encourage platforms to monitor their sites and provide families with protection. It felt that the only way to do so was to protect them from responsibility for third parties’ material on their sites.

After months of negotiation, the Conference Committee introduced the Telecommunications Act of 1996 in February of 1996. This Act demonstrated the synergy between the Senate’s CDA and the House’s IFFE. Title V of the Telecommunications Act is entitled Obscenity and Violence. Under this subtitle is the Short Title, The Communications Decency Act of 1996. This Section is the result of this compromise. The purpose of the

⁴³Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, UNIV. RICH. J. L. AND TECH., 64 (2020) (Its sponsor has also argued it was important to respond to Stratton Oakmont because “common law extended no protections to platforms that moderate user content.”); *Stratton Oakmont v. Prodigy Servs. Co.*, 1995 WL 323710, *1 (Sup. Ct. May 24, 1995).

⁴⁴141 CONG. REC. S8089 (daily ed. June 9, 1995) (comments Sen. Exon) (“The computer is a wonderful device for arranging, storing, and making it relatively easy for anyone to call up information or pictures on any subject. That is part of the beauty of the Internet system.”).

Telecommunications Act is to update the 1934 Communications Act,⁴⁵ and in so doing Congress saw fit to include child protective components. The effort was bipartisan, included the White House, and reflected a reconciliation of both bills.⁴⁶ The Committee Report listed as a resolved issue “cyberporn: requires operators of computer networks to screen out indecent material for children; carriers of indecent material will not be liable for the content of information generated by others....”⁴⁷

Although Congressman Cox has since asserted that he never intended §230 as an amendment to the CDA, that is exactly how it sits within the law as it emerged from Conference. Furthermore, the debate around the legislation reflects that Title V- which houses these IFFE concepts as a component of the CDA - has a child protection landscape.⁴⁸ To be sure, the Telecommunication Act of 1996 has many goals within its 107 pages.⁴⁹ But much of the debate around Title V makes clear that proponents and opponents alike understood it to possess child protection elements.⁵⁰ Senator Grassley described the bill as “a needed step in protecting children from child molesters and unscrupulous porn merchants,” noting the need for federal

⁴⁵141 CONG. REC. S2009 (daily reg. Feb. 1, 1996) (comments of Sen. Pressler).

⁴⁶141 CONG. REC. S2010 (daily reg. Feb. 1, 1996); *see also* 142 CONG. REC. 1993, 2042 (comments of Sen. Breaux) (“there is no doubt about it. This conference Report was crafted in a bipartisan, I think non-partisan, manner.”).

⁴⁷141 CONG. REC. S2011, ¶ 11.

⁴⁸Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, UNIV. RICH. J. L. AND TECH., 64 (2020) (One argument Cox offers to support his claim that Section 230 is not part of the CDA is that when two provisions of the CDA were found vague by the Supreme Court no efforts were made to resurrect them. Given the number of years it took Congress to update telecommunications law, the fact that no one sought to add provisions hardly seems to lead to this conclusion. Even if so, the last two Congressional terms had dozens of bills to amend or repeal §230. Moreover, when the Senate was actually debating the Conference Report, one Senator noted that “the Internet indecency provisions have met with the barest of resistance in this Chamber.”); 142 CONG. REC. 1993, 2036 (comments of Sen. Feingold).

⁴⁹142 CONG. REC. 1993, 2041 (comments of Sen. Exon) (“Concurrent with our efforts to make the Internet and other computer services safe for families and children, this bill includes legislation which will help turn the information revolution to the benefit of all Americans, but especially America’s children.”).

⁵⁰*E.g.*, 142 CONG. REC. 1993, 2013 (comments of Sen. Stevens) (noting this is not a deregulation bill); *see also, id.* at 2030 (comments of Sen. Coats) (“Perhaps most importantly this bill will help protect children from computer pornography which today is readily accessible on the internet.”).

legislation in this area, not just new technologies.⁵¹ Another Senator noted that “the Conference Report contains strong protections for America’s children.”⁵² Senator Coats again discussed the linkage between the bill and protecting children from not only pornography but “images and text dealing with the sexual abuse of children....”⁵³

Opponents to the bipartisan compromise legislation also debated the bill in part within the context of child protection. Senator Leahy acknowledged that “[a]ll of us 100 members of the U.S. Senate oppose the idea of child pornography,” but expressed his constitutional concerns about two provisions of the CDA outside §230.⁵⁴ Senator Feingold discussed the legislation as redundant to current federal laws regarding child abuse, stating that “much of what the proponents of this legislation wish to banish from cyberspace is already subject to criminal penalties – obscenity, child pornography, and child exploitation via computer networks are already criminal acts.”⁵⁵

As the Chief Judge of the Second Circuit has since noted, §230 was unquestionably a statute concerned with child protection. “Of the myriad of issues the emerging Internet implicated, Congress tackled only one: the ease with which the Internet delivers indecent and offensive material, especially to minors.” He also rejected claims such as those of Representative Cox, that §230 has nothing to do with the CDA. The “Conference Committee had two alternative versions for countering the spread of indecent online material to minors. The Committee chose not to choose. Congress instead adopted both amendments as part of the final

⁵¹142 CONG. REC. 1993, 2029 (comments of Sen. Grassley).

⁵²142 CONG. REC. 1993, 2030 (comments of Sen. Holmes).

⁵³142 CONG. REC. 1993, 2030 (comments of Sen. Coats).

⁵⁴142 CONG. REC. 1993, 2015 (comments of Sen. Leahy).

⁵⁵142 CONG. REC. 1993, 2035 (comments of Sen. Feingold).

Communications Decency Act.”⁵⁶ He insightfully observed that this was not coincidence, acknowledging that Congress removed from the Cox/Wyden approach the provisions to deny the FCC the jurisdiction to regulate the Internet.⁵⁷ Therefore, consistent with the legislative history of Title V, Congress passed §230 as part of the CDA, and part of a larger discussion regarding the pathways to prevent to distribution of sexually explicit material which would include CSAM.

D. The Text of Section 230 Itself Reflects this Legislative History of a Statute Emerging from a Landscape that Includes Child Protection

In the Telecommunications Act, Congress placed the relevant legislation within Title V (Obscenity and Violence), Subtitle A (Obscene, Harassing, and Wrongful Utilization of Telecommunications Facilities), and the short title, The Communications Decency Act of 1996.⁵⁸ Additionally, Congress renamed the relevant provision: *Protection for Private Blocking and Screening of Offensive Material*. From the original text, §230 includes five statements of the policy of the United States. The first two speak to the preference for an open and robust Internet with limited government regulation.⁵⁹ The remaining three policies speak to the importance of technologies to afford individuals and institutions control over the information that reaches children and the ability to restrict children’s access to objectionable material.⁶⁰ Among those, the statute explicitly states that it is the policy of the United States to “ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, and harassment by means of a computer” – the very concerns mentioned in the CDA debates.⁶¹ The inclusion of these policies, combined with the text of the provision that explicitly states the

⁵⁶Force v. Facebook, 934 F.3d 53 (2d Cir. 2019) (Katzmann, CJ dissenting).

⁵⁷Force v. Facebook, 934 F.3d 53 (2d Cir. 2019) (Katzmann, CJ dissenting).

⁵⁸Pub L. 104, Telecommunications Act of 1996, Title V.

⁵⁹47 U.S.C. § 230(b)(1), (2).

⁶⁰47 U.S.C. § 230(b)(3), (4).

⁶¹47 U.S.C. § 230(b)(5).

statute should have no effect on enforcement of obscenity and child exploitation federal criminal law,⁶² reflect the climate from which §230 came: a debate that included discussion about the best methods to protect children from explicit material and sexual exploitation.

Critical to the supporters of IFFE, §230 includes language providing what was intended to be limited immunity. As the title suggests, the first immunity includes protection from civil liability for “Good Samaritan” *blocking or screening* of offensive material made in good faith.⁶³ What Congress meant by “offensive material” is explicitly defined in the statute: “material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not the material is constitutionally protected.”⁶⁴ Further regarding limited immunity, this provision also states that ICS’s shall not be treated as publishers for information provided by a third party.⁶⁵ In a traditional context, a publisher is responsible for the information it prints. Supporters of IFFE did not want that liability for platforms that merely disseminate content from third parties.⁶⁶ Section 230(c) (1), therefore, precludes liability for information a user disseminates on an ICS’s platform, provided the ICS is not the content creator in whole or in part.⁶⁷

Again, this focus on sexually exploitive content reflects Congressional intent to protect children. Furthermore, the legislation explicitly states that it will not affect the enforcement of

⁶² 47 U.S.C. § 230(e) (“Nothing in this section shall be construed to impair the enforcement of section [223](#) or [231](#) of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.”).

⁶³ 47 U.S.C. § 230(c)(2).

⁶⁴ 47 U.S.C. § 230(c)(2).

⁶⁵ 47 U.S.C. § 230(c)(1).

⁶⁶ *Doe v. America Online*, 783 So.2d 1010, 1019 (Fla. 2001), (Lewis, J. in dissent) (One judge characterized this as Congress intending for ICS to be treated as distributors and not publishers.).

⁶⁷ *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1165 (9th Cir. 2008); *Malwarebytes, Inc. v. Enigma Software*, 592 U.S. ____ (2020) (Thomas, J.).

any criminal statute, but also specifically mentions laws relating to obscenity and the sexual exploitation of children.⁶⁸

This text, reflecting many priorities, explicitly includes in those priorities child protection. The understanding of the plain language of the text is supported by the Report's discussion concerning the CDA and IFFE relating to their goals of developing the most effective methods to protect children. The Conference Report states:

This Section [§230] provides 'Good Samaritan' protections from civil liability for providers or users of interactive computer services for actions to restrict or enable restrictions of access to objectionable material online....The conferees believe such decisions [like Stratton Oakmont] create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.⁶⁹

One of the authors of IFFE now argues 24 years later that §230 should not be interpreted as part of the Communications Decency Act.⁷⁰ Additionally, he asserts the legislation was conceived of without industry lobbying or support. Not only are those assertions belied by the aforementioned legislative history but also by contemporary media coverage as well.

News coverage at the time of these discussions characterized the CDA and IFFE as different approaches to the same issue of addressing explicit material. The Washington Post described IFFE as providing a system free of government regulation only "if they [ICS's] take steps to control smut."⁷¹ The Washington Post further documented what is now §230 as an effort by the Industry to create an alternative way to protect children. "The issue has been fueled

⁶⁸47 U.S.C. § 230(e)(1).

⁶⁹S. REP. NO. 104-230 at 194 (1996).

⁷⁰Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, UNIV. RICH. J. L. AND TECH., 64 (2020).

⁷¹Daniel Pearl, *House Leaders Seek Other Ways To Fight Smut on Internet*, WALL ST. J., June 21, 1995, at B2.

by several high profile incidents involving minors on the popular services that allowed people to link their computers to others via telephone lines. Since users can trade text, pictures, and sounds, there has been a proliferation of sexually oriented areas where people can ‘chat’ or obtain explicit photographs.”⁷² Critical here is not that these were different approaches but that they were both approaches to address the problem of, inter alia, child protection from exploitation. The New York Times agreed these were proposals from different perspectives, but both “intended to shield children from pornography in words and pictures as well as from other material deemed objectionable that is distributed over the Internet.”⁷³

Therefore, the media coverage reflects that Congress considered two different approaches to the problem of explicit content within the emerging medium and Congress ultimately combined them to utilize both federal law and business incentives to most effectively protect children. For this issue regarding telecommunication and the Internet, the dispute was not whether to protect children, but how to do so. The Senate initially proposed doing so in a number of ways from scrambling channels on cable television to criminal liability at the point of dissemination on the Internet.⁷⁴ The House articulated two main reasons for advancing its approach. First, it believed “indecent” was too vague a label and raised constitutional concerns.⁷⁵ Many members preferred an approach that protected children at the point of receipt rather than criminalize the point of distribution. This view encouraged, indeed promised, tech

⁷²Kara Swisher and Elizabeth Corcoran, *Gingrich Condemns On-Line Decency Act*, WASH. POST, June 22, 1995, at D8.

⁷³Steve Lohr, *Conservatives Split On How To Regulate The Internet*, N. Y. TIMES, Dec. 4, 1995.

⁷⁴Nicolas Conlon, *Freedom Filter Versus User Control: Limiting Scope of Section 230(c)(2) Immunity*, 2014 UNIV. ILL. J. L. TECH. & POL’Y. 105, 114 (2014).

⁷⁵*Reno v. A.C.L.U.*, 521 U.S. 844, 874 (1997) (This later proved to be correct as Congress created an avenue for immediate appeal and the Supreme Court found this specific “indecent” language too broad.).

companies would produce workable technologies that would allow parents and users to filter out such material.⁷⁶ The passage of §230 was, in part, based on that language.

Therefore, the Conference, and ultimately Congress incorporated both approaches into the final bill, placing them together under the Communications Decency Act. It prohibited both the illegal transmission of such material, but also accepted the promise from the industry that they would accept the incentive to develop parental controls and filters early access to the public.⁷⁷ Indeed this was the vision of one of the members of the Conference and author of the CDA who advocated that both federal law and technological solutions were needed to protect children.⁷⁸

This history makes clear that §230 has incorrectly been re-characterized as a stand-alone piece of legislation designed solely to promote an unregulated Internet.⁷⁹ To the contrary, Congress took the original legislation that became §230 and amended it to the CDA to provide both a statutory effort to protect children as well as an incentive for future CSP's to develop technologies to protect children and not be civilly sued for doing so.

E. The Promises of §230's Proponents

Even if one rejects returning §230 to its roots which include child protection, there remains a need to revisit it consistent with its promise. In addition to the Conference

⁷⁶Steve Lohr, *Conservatives Split on How to Regulate the Internet*, N. Y. TIMES, Dec. 4, 1995 (“Both camps agree on the need to protect children from offensive material on computer networks. But the methods they advocate represent two divergent views on how to regulate the fast-growing medium.”).

⁷⁷Nicolas Conlon, *Freedom Filter Versus User Control: Limiting Scope of Section 230(c)(2) Immunity*, 2014 UNIV. ILL. J. L. TECH. & POL’Y. 105, 115 (2014).

⁷⁸Kara Swisher, *Ban On Online Smut Opposed*, WASH. POST, July 18, 1995, at D3; The Wall Street Journal described how the tech industry and law makers worked on a compromise, describing several proposals that were being considered including changing “indecent” to “harmful to minors,” and credit card verification. Indeed, the Part 1, notes for services that take “reasonable, effective, and appropriate steps to screen material.”

⁷⁹ See, Part I, notes 17-21.

Committee's position, those who advocated for IFFE did so with the promise that that system would allow for the tech industry to develop all the technology needed to protect children from explicit and exploitive imagery. Congressman Cox asserted that a deregulated environment with immunity would remove any deterrence for companies to develop software because of a decision such as Stratton Oakmont. Although that technology did not exist, the tech industry was more than happy to claim it would develop it and it would become more sophisticated and easily available to parents.⁸⁰

Contemporary news accounts demonstrate the promises made by tech companies about the ability of what would become §230 to protect children. The Washington Post reported that tech companies promised to provide and utilize technology to filter out such material.⁸¹ These representations were not inconsequential statements. Rather, they were part of an intensive lobbying effort. Not only did the industry claim this verbally. The New York Times noted, "Interactive Services Association, a trade group for the on-line industry that supports the Cox-Wyden Amendment demonstrated for the staff members of the conferees on the telecom bill 'software that can filter material deemed objectionable.'"⁸² The Washington Post described how "[o]n-line companies, software makers, and civil liberties groups came to Capitol Hill yesterday to make their case that the on-line world can be made safe for children without government intervention."⁸³ The result of this effort was described as one in which some "reject[ed] promises from the on-line industry that companies like America Online and Netscape Communications Corporation would give parents tools to screen offensive material if they could

⁸⁰Robert Corn-Revere, *New Age Comstockery*, 4 COMM. L. CONCEPTUS 173, 174 (1996).

⁸¹Kara Swisher and Elizabeth Corcoran, *Gingrich Condemns On-Line Decency Act*, WASH. POST, June 22, 1995, at D8.

⁸²Steve Lohr, *Conservative Split On How To Regulate The Internet*, N. Y. TIMES, Nov. 9, 1995.

⁸³E.g., Kara Swisher, *Ban On Online Smut Opposed*, WASH. POST, July 18, 1995, at D3.

be sure such actions wouldn't make them liable for a message sent by a subscriber.”⁸⁴ The rejections were prophetic. The Department of Justice recently shared that sentiment by concluding that this “expansive statutory interpretation combined with technological developments has decreased the incentives of online platforms to address illicit activity on their services.”⁸⁵ That is exactly the opposite of what was promised by 230's proponents.

F. Scholars Describe the CDA as Enacted With §230 As Related to Child Protection

Many scholars and commentators note that Title V of the Telecommunications Act focusses on many issues, including child protection. “Congress enacted the Communications Decency Act of 1996 in an attempt to prevent minors from gaining access to sexually explicit material on the Internet.”⁸⁶ The resulting Title V emerged out of the compromise between the original Communications Decency Act and the House proposal.⁸⁷ “The Communications Decency Act's stated purpose is to protect children from access to indecent and obscene materials over the Internet....”⁸⁸

The commentators noted that the differences between the House and Senate bills were resolved in conference “with significant lobbying from both sides. A Coalition of online service providers, common carriers and computer companies supported a compromise bill...based primarily on the Cox/Wyden amendment but allowing more targeted criminal penalties.”⁸⁹ The

⁸⁴Daniel Pearl, *Compromise Sought On Curbs For The Internet*, Wall St. J., Dec. 4, 1995.

⁸⁵ See also *Department of Justice's Review of Section 230 of the Communication Decency Act Of 1996*, Dep't. of Just. Archives, <https://www.justice.gov/archives/ag/departments-justice-s-review-section-230-communications-decency-act-1996>.

⁸⁶Sara Ziegler, *The Communications Decency Act of 1996*, FIRST AMEND. ENCYCLOPEDIA (2009), <https://www.mtsu.edu/first-amendment/article/1070/communications-decency-act-of-1996>.

⁸⁷E.g., Robert Corn-Revere, *New Age Comstockery*, 4 COMM. LAW. CONSPECTUS 173, 174 (1996).

⁸⁸E.g., Lorraine Mercier, *The Communications Decency Act, Congress's First Attempt to Sensor Speech Over the Internet*, 9 LOY. CONSUMER L. REV. 274, 275 (1997); Danielle Keats Citron and Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans S 230 Immunity*, 86 Fordham L. Rev. 401, 406 (2017).

⁸⁹Robert Corn-Revere, *New Age Comstockery*, 4 COMM. L. CONSPECTUS 173, 175 (1996).

final version has been described as dropping the Cox/Wyden proposal to explicitly prohibit FCC regulation, but adopting their concept to reshape the CDA. The conference Committee voted to keep the indecency standard and the “Cox/Wyden bill was retained in the final Telecommunications act, but only as a limitation on civil liability.”⁹⁰ Criminal liability explicitly remained in the bill.

As will be discussed *infra*, ICS’s and tech companies have asserted that these provisions provide broad immunity, not the narrow one articulated in the texts itself. This claim by ICS’s of broad immunity has turned §230 on its head, ignoring the immunity was intended to protect children not be a defense when they are harmed by inaction. “The House Rules Committee, which allowed consideration of the Cox-Wyden amendment, described that provision as “protecting from liability those providers and users seeking to clean up the Internet. The final version of § 230 of the CDA reflects [the] policy objective, not a broader objective of immunizing platforms for destructive third-party content they encourage or intentionally tolerate.”⁹¹ Scholars clearly recognize that among the purposes of §230, protection of children was clear. Citron and Franks describe §230 as “a provision originally designed to encourage tech companies to clean up “offensive” online content... federal lawmakers wanted the internet to be open and free, but they also realized that such openness risked encouraging noxious activity.”⁹²

⁹⁰Robert Corn-Revere, *New Age Comstockery*, 4 COMM. L. CONCEPTUS 173, 175 (1996)(emphasis added).

⁹¹Danielle Keats Citron and Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans S 230 Immunity*, 86 FORDHAM L. REV. 401, 406 (2017). *See also*, Department of Justice’s Review of Section 230 of the Communication Decency Act Of 1996, Dep’t. of Just. Archives, <https://www.justice.gov/archives/ag/departments-justice-s-review-section-230-communications-decency-act-1996> (“Congress originally enacted the statute to nurture a nascent industry while also incentivizing online platforms to remove content harmful to children.”).

⁹² Danielle Keats Citron & Mary Anne Franks, *The Internet as A Speech Machine and Other Myths Confounding Section 230 Reform*, 2020 U. Chi. Legal F. 45, 45–46 (2020).

II. Notwithstanding This Inclusion of Child Protection Among §230's Purposes, Courts Initially Ignored That Purpose

As discussed *supra*, the CDA had many components addressing various aspects of telecommunications including the Internet. While, for some lawmakers, the criminalization of ICS's dissemination of explicit material was a problematic regulation, even for supporters of IFFE the concept of limited access to sexually explicit material was not objectionable. Although it is axiomatic that the protection of children is a legitimate government interest,⁹³ the opponents to the CDA expressed concern regarding two CDA provisions outside of §230. Specifically, that 47 U.S.C. 223(a)(1)(B)'s prohibition of "indecent" transmission and 223(d)'s "patently offensive" material utilized such broad terms that they would not survive constitutional challenges.⁹⁴ While obscenity and CSAM/child pornography have understood definitions which have withstood constitutional scrutiny,⁹⁵ "indecent" and "offensive" did not. Consequently, Congress allowed for expedited judicial review and the Supreme Court found those two provisions vague.⁹⁶ In so doing, the Court went out of its way to limit its ruling to those two provisions by severing the problematic terms and allowing the prohibition of disseminating obscene material because obscene material may be constitutionally banned.⁹⁷

This ruling had nothing to do with §230 or the legislative intent of this provision. However, after that point, the scope of the immunity provisions of §230 began to be litigated. The course of this jurisprudence is tortured and initially turned the intended limited immunity on its head.⁹⁸ This was in part due to an unbalanced and, therefore, inaccurate focus on the non-

⁹³ *Pacifica v. FCC Found.*, 438 U.S. 726, 726 (1978).

⁹⁴ *E.g.*, 142 CONG. REC. 1993, 2036 (comments of Sen. Feingold).

⁹⁵ *Miller v. California*, 413 U.S. 15 (1973); *New York v. Ferber*, 458 U.S. 747 (1982); *Osborne v. Ohio*, 495 U.S. 103 (1990).

⁹⁶ *Reno v. A.C.L.U.*, 521 U.S. 844, 874 (1997).

⁹⁷ *Reno v. A.C.L.U.*, 521 U.S. 844, 882-83 (1997).

⁹⁸ For a comprehensive discussion of this jurisprudence as it relates to sex trafficking *see* Mary Graw Leary, *The Indecency of the Communication Decency Act*, 41 Harv. J. L. Pub. Pol'y 553, 574-581 (2018).

child protective purposes of §230. This became problematic as these precedents were applied to child exploitation cases, creating a near *de facto* absolute immunity. However, more recently courts have acknowledged the context in which §230 was created, and resisted this evolution. Similarly, Congress has legislatively corrected this jurisprudence in narrow legislation regarding sex trafficking.⁹⁹

Notwithstanding the limited immunity intended for §230, the first case to litigate this question – a defamation case – set a course of jurisprudence that pulled §230 from its moorings. In *Zeran v. America Online*,¹⁰⁰ the Fourth Circuit addressed the defamation liability for the internet service provider, America Online (AOL). In so doing, the court focused on the policies of §230 relating to freedom from regulation and tort liability.¹⁰¹ In one sense this seemed sufficient, as that initial case did not raise child protection and exploitation issues and reference to these purposes seemed unnecessary. However, it then made the following broad statement, “Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, *in part*, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.”¹⁰² Notably, the court qualified its description of the purpose of §230 by using the term “in part.” However, it never explained the other purposes of §230 which demonstrate the very limited immunity §230 provides and that qualifier has largely been ignored.

⁹⁹ Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Public Law No: 115-164 (04/11/2018).

¹⁰⁰ *Zeran v. Am. Online, Inc.*, 129 F.3d 327 (4th Cir. 1997).

¹⁰¹ *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997).

¹⁰² *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) (emphasis added).

Rather, the court went on to describe the immunity in this defamation case – a classic publishing issue- as “broad.” While it correctly referred to Congress’s intent to overturn Stratton Oakmont, it seemed to de-emphasize all the other goals of §230 within the CDA. This reasoning, however, took on a life of its own, and only in recent years – in the current context of the Internet – have courts and Congress acknowledged the error of this path.¹⁰³

Notwithstanding the legislative history and text which outlines an intended narrow immunity for Good Samaritans and for ICS’s to not be treated as publishers, caselaw referred to this early defamation case to provide broad *de facto* absolute immunity in many cases involving children.¹⁰⁴ For example, although the CDA explicitly focused on child pornography, the court in *Doe v. America Online, Inc.*, embraced this concept of broad immunity.¹⁰⁵ In that case, the plaintiff argued that AOL was not a publisher, but a distributor of CSAM. It accused AOL of knowingly distributing and allowing advertisements for child pornography, negligence, and a failure to respond to notification that its services were being utilized to distribute obscene material. The Florida court’s majority rejected that argument, extending *Zeran’s* assertion that websites are not distributors for nearly any claim made against them.¹⁰⁶

The majority’s analysis in *Doe*, however, is very troubling and inconsistent with §230. Although the case involved allegations regarding CSAM, the majority did not focus its reasoning on the purposes of §230 consistent with those priorities regarding explicit material and exploitation. Rather, the court quoted *Zeran* heavily, and thus helped perpetuate a broad

¹⁰³ *E.g.*, Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008); Jane Doe #1 v. MG Freesites, Ltd., No. 7:21-cv-00220-LSC, 2022 U.S. Dist. LEXIS 23199 (N.D. Ala Feb. 9, 2022).

¹⁰⁴ Jane Doe #1 v. MG Freesites, Ltd., No. 7:21-cv-00220-LSC, 2022 U.S. Dist. LEXIS 23199 (N.D. Ala Feb. 9, 2022).

¹⁰⁵ *Doe v. Am. Online*, 783 So. 2d 1010 (Fla. 2001).

¹⁰⁶ *Doe v. Am. Online*, 783 So. 2d 1010 (Fla. 2001).

definition of publisher and that the sole purpose behind §230 of the CDA was an unregulated Internet.¹⁰⁷

Judge Lewis, writing in dissent, forewarned of the error in the majority's over reliance on Zeran.

Contrary to the majority's view, however, the carefully crafted statute at issue, undergirded by a clear legislative history, does not reflect an intent to totally exonerate and insulate an ISP from responsibility where, as here, it is alleged that an ISP has acted as a knowing distributor of material leading to the purchase, sale, expansion and advancement of child pornography....¹⁰⁸

He found the majority's blind following of Zeran "frustrate[d] the core concepts explicitly furthered by the Act and contravene[d] its express purpose [T]he so-called Decency Act has, contrary to well established legal principles been transformed from an appropriate shield into a sword of harm."¹⁰⁹ He forewarned this would create "carte blanche immunity for wrongful conduct plainly not intended by Congress."¹¹⁰

Judge Lewis's effort to scrutinize the actual intent of §230, however, was not repeated by many courts. While some cases sought to return interpretations of §230 to its original intent,¹¹¹ Zeran's reference to "broad immunity" was embraced by tech companies and asserted in numerous courts who seemed to repeat it with little effort to review the legislative history in full.

¹⁰⁷ Doe v. Am. Online, 783 So. 2d 1010, 1019 (Fla. 2001); *see also* Mary Graw Leary, *The Indecency of the Communication Decency Act*, 41 Harv. J. L. Pub. Pol'y 553, 574-581 (2018).

¹⁰⁸ Doe v. Am. Online, 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J. in dissent).

¹⁰⁹ Doe v. Am. Online, 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J. in dissent).

¹¹⁰ Doe v. Am. Online, 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J. in dissent).

¹¹¹ J.S. v. Vill. Voice Media Holdings, 359 P.3d 714 (Wash. 2015) (en banc); Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008).

This has led to immunity from more and more claims having little to do with publishing such as terrorism,¹¹² refusal to follow court orders,¹¹³ and illegal firearms sales¹¹⁴ to name a few.

This pattern reached a crescendo, however, in 2016. In *Jane Doe No. 1 v. Backpage.com, LLC*,¹¹⁵ plaintiffs – sex trafficking survivors who were repeatedly sold on Backpage.com, accused defendants of entering into a joint venture with sex traffickers wherein Backpage adapted posting requirements, accepted anonymous payments, advised traffickers how to avoid law enforcement, and stripped images of metadata – all to facilitate sex trafficking.¹¹⁶ None of these actions remotely resembled traditional publishing duties. Furthermore, since the passage of the CDA, Congress passed the Trafficking Victims Protection Reauthorization Act which afforded victims an explicit private right of action to civilly sue those who facilitated their trafficking, as did the Massachusetts state legislature.¹¹⁷ Yet, citing to the very early § 230 cases from the early 2000’s, the First Circuit adopted, without analysis, the preference “for broad construction” of §230 while at the same time characterizing this liberal construction as “a capacious conception of what it means to treat a website operator as the publisher or speaker of information provided by a third party.”¹¹⁸ With that broad interpretation of the narrowly written CDA, the First Circuit then concluded that the plaintiffs' claims under the TVPA were, in fact, ones that treated Backpage.com as a publisher.¹¹⁹

¹¹² *Force v. Facebook*, 934 F.3d 53 (2d. Cir. 2019).

¹¹³ *Hassell v. Bird*, 420 P.3d 776, 789 (Cal. 2018) (Yelp’s refusal to comply with a court injunction is protected by Section 230).

¹¹⁴ *Daniel v. Armslist, LLC*, 926 N.W.2d 710, 715, 726 (Wis. 2019), cert. denied. 140 S.Ct. 562 (2019) (website was immune under Section 230, despite allegations that website intentionally designed to evade federal firearm laws).

¹¹⁵ *Doe v. Backpage.com, LLC*, 817 F.3d 12, 16-21 (1st Cir. 2016).

¹¹⁶ *Doe v. Backpage.com, LLC*, 817 F.3d 12, 16-21 (1st Cir. 2016).

¹¹⁷ *Doe v. Backpage.com, LLC*, 817 F.3d 12, 16-21 (1st Cir. 2016).

¹¹⁸ *Doe v. Backpage.com, LLC*, 817 F.3d 12, 18-19 (1st Cir. 2016).

¹¹⁹ *Doe v. Backpage.com, LLC*, 817 F.3d 12, 22 (1st Cir. 2016).

If that were not a shocking enough twist of the intended limited immunity of §230, the court went even further in addressing the victims' TVPRA claims:

[E]ven if we assume, for argument's sake, that Backpage's conduct amounts to "participation in a [sex-trafficking] venture"--a phrase that no published opinion has yet interpreted--the TVPRA claims as pleaded premise that participation on Backpage's actions as a publisher or speaker of third-party content. The strictures of Section 230(c) foreclose such suits.¹²⁰

Such a holding perverted the intended limited immunity provision of §230 – an immunity provision with roots in an effort to protect children from sexual exploitation. Congress finally accepted the invitation of the First Circuit to clarify the scope of this 1996 immunity provision as it related to the private right of action Congress created in 2000.¹²¹ The United States Senate engaged in a two year investigation and issued a Report entitled *Backpage's Knowing Facilitation of Sex Trafficking* which recounted allegations of sex trafficking and conspiracy to engage in sex trafficking by the ICS Backpage.com.¹²² Moreover, for the first time in nearly two decades, Congress finally bent to pressure and amended §230 to include sex trafficking among the crimes that are carved out of §230 immunity – a point that seemed obvious to all those who voted on the immunity in 1996.¹²³ It allowed for state enforcement of state criminal laws prohibiting sex trafficking and for federal civil suits authorized through 18 U.S.C. 1595. All these avenues had previously been closed to sex trafficking victims trafficked on online platforms, thus preventing access to justice for thousands of victims.

¹²⁰Doe v. Backpage.com, LLC, 817 F.3d 12, 21 (1st Cir. 2016) (footnote omitted); Notably, "participation in a [sex trafficking] venture" is expressly criminalized by 18 U.S.C. § 1591(a)(2).

¹²¹ Doe v. Backpage.com, LLC, 817 F.3d 12, 21 (1st Cir. 2016) ("If the evils that the appellants have identified are deemed to outweigh the First Amendment values that drive the CDA, the remedy is through legislation, not through litigation.").

¹²² *Backpage.com's Knowing Facilitation of Online Sex Trafficking: Hearing Before the Subcomm. on Investigations*, 115th Cong. (2017) (The CEO of Backpage eventually plead guilty to numerous criminal offenses including conspiracy to engage in human trafficking.).

¹²³ Allow States and Victims to Fight Online Sex Trafficking Act, Pub. L. No. 115-164, 132 Stat. 1253 (2018).

Notably, however, this previous line of cases manifests the breadth the immunity provision has taken – even preventing states from enforcing their own criminal laws. For example, §230 provides that “Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.”¹²⁴ Tech companies successfully argued that this language prevented states from enforcing state human trafficking laws against ICS’s, although such was never the intent. Even according to its sponsor, Representative Cox, this passage was to limit state development of their own Internet policy, not to limit the enforcement of state criminal law.¹²⁵ As the Department of justice noted, “[t]he combination of significant technological change since 1996 and the expansive interpretation that courts have given §230...has left online platforms immune for a wide array of illicit activity on their services.”¹²⁶

In recent years, more courts and individual judges have questioned the perversion of §230 immunity from the intended limited immunity to near de facto complete immunity. The Washington State Supreme Court was the first court that allow a sex trafficking case proceed past the motion to dismiss stage on state law grounds.¹²⁷ In so doing it seemed to accept the conventional understanding of a rather broad immunity, but recognized the *Roommates*’ conclusion that a website can be both a content provider and an interactive computer service. Thus, it concluded that many of the claims “alleged facts that, if proved true,

¹²⁴ 47 U.S.C.A. § 230(e)(3).

¹²⁵ Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, UNIV. RICH. J. L. AND TECH., 64 (2020) (describing this section as “consistent with robust enforcement of state crimes.”).

¹²⁶ *Department of Justice’s Review of Section 230 of the Communication Decency Act Of 1996*, Dep’t. of Just. Archives, <https://www.justice.gov/archives/ag/departments-justice-s-review-section-230-communications-decency-act-1996>.

¹²⁷ *J.S. v. Vill. Voice Media Holdings*, 359 P.3d 714 (Wash. 2015) (en banc).

would show that Backpage did more than simply maintain neutral policies prohibiting or limiting certain content.”¹²⁸

Perhaps as important was the concurring opinion of Justice Wiggins. Justice Wiggins, who wrote separately to clarify that plaintiffs' claims did not treat Backpage as a publisher or speaker and to vehemently rejected Backpage and the dissent's view that § 230 provides immunity to such actions by a platform.¹²⁹ “Subsection 230(c)(1) ... provides a narrower protection from liability: the plain language of the statute creates a defense when there is (1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker of information (3) that is provided by another information content provider. Thus, when the cause of action does not treat an intermediary as a publisher or speaker, subsection 230(c) (1) cannot be read to protect that intermediary from liability.”¹³⁰

Similarly, Chief Justice Katzmman, writing in the dissent in *Force v. Facebook*, also challenged the majority opinion's granting of immunity in an anti-terrorism civil suit.¹³¹ He noted that §230 “was designed to encourage computer service providers to shield minors from obscene material so that it now immunizes those same providers for allegedly connecting terrorists to one another.”¹³² Such a view should not be considered novel, as there should be no dispute as to the narrow scope of the immunity. The legislative history and text convey that. Even its sponsor stated that “it is firmly established in the caselaw that §230 cannot act as a

¹²⁸ J.S. v. Vill. Voice Media Holdings, 359 P.3d 714, 717 (Wash. 2015) (en banc).

¹²⁹ J.S. v. Vill. Voice Media Holdings, 359 P.3d 714, 718 (Wash. 2015)(Wiggins, J., concurring).

¹³⁰ J.S. v. Vill. Voice Media Holdings, 359 P.3d 714, 718-19 (Wash. 2015)(Wiggins, J., concurring).

¹³¹ *Force v. Facebook*, 934 F.3d 53, 77 (Katzmman, C.J., dissenting).

¹³² *Force v. Facebook*, 934 F.3d 53, 77 (Katzmman, C.J., dissenting).

shield when encouraging a website to be in any way complicit in the creation or development of illegal content.”¹³³

Most recently, Justice Thomas lamented the current state of jurisprudence regarding §230 in a statement accompanying a denial of a petition for writ of certiorari.¹³⁴ In *Malwarebytes, Inc. v. Enigma Software Group USA, LLC*, Justice Thomas agreed with the denial of certiorari, but wrote separately to invite reconsideration of whether the actual text of §230 “aligns with the current state of immunity enjoyed by Internet platforms.”¹³⁵ Returning to the actual intent and text of Congress in 1996, he described the immunity as a “limited protection [that] enables companies to create community guidelines and remove harmful content without worrying about legal reprisal.”¹³⁶ He summarized the roots of the law as responding to Stratton Oakmont and correcting an increased liability for acting to protect children by noting two effects. He stated §230(c) (1) does not make an ISP a publisher by simply hosting third party content and §230(c)(2)(A) provides immunity when companies take good faith steps to decrease access to objectionable material.¹³⁷

This modest understanding is a **far cry from what has prevailed in court. Adopting the too-common practice of reading extra immunity into statutes where it does not belong,** courts have relied on policy and purpose arguments to grant **sweeping** protections to Internet platforms.¹³⁸

¹³³ Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, U. OF RICHMOND J. L. AND TECH. (Aug. 27, 2020), <https://jolt.richmond.edu/2020/08/27/the-origins-and-original-intent-of-section-230-of-the-communications-decency-act/>.

¹³⁴ *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13 (2020).

¹³⁵ *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 2 (2020).

¹³⁶ *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 2 (2020).

¹³⁷ *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 2 (2020).

¹³⁸ *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 4 (2020) (citations omitted).

He questioned this approach for several reasons, not the least of which that §230 was part of the CDA which made it a crime to knowingly display even third party obscene content to a minor.¹³⁹ He further notes that if Congress intended to eliminate publisher and distributor liability, it would have done so explicitly.¹⁴⁰

Of particular concern to Justice Thomas was the trend in courts departing from §230 text. “Courts have done so by awarding immunity for their own content in contrast to §230(c)(1) and eviscerating the narrower liability” of §230(c)(2)(A).¹⁴¹ He then focused on particularly exploitive cases including ones involving sex trafficking and, importantly, CSAM.¹⁴²

Of significance, however, Justice Thomas understands the practical consequences of immunity. It precludes victim survivors’ access to court because it allows a defendant to file a motion to dismiss prior to discovery. As such, victim survivors are never afforded the opportunity to prove their allegation is court in a substantive way. “Paring back the sweeping immunity, courts have read into §230 would not necessarily render defendants liable for online

¹³⁹ *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 5 (2020) (“It is odd to hold, as courts have, that Congress implicitly eliminated distributor liability in the very Act in which Congress explicitly imposed it.”).

¹⁴⁰ *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 6 (2020).

¹⁴¹ *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 7 (2020) (Justice Thomas raised concerns about a Second Circuit case in which the court affirmed the dismissal of a complaint against Facebook by victims of terrorist attacks who accused Facebook of using its algorithm to connect terrorists to one another in violation anti-terrorism laws.); *Force v. Facebook*, 934 F.3d 53 (2nd Cir. 2019) (Notably Force both recognized the purpose of the CDA “as to protect children from sexually explicit conduct,” but then went on to note that §230 was enacted to “maintain the robust nature of Internet communications” and conclude that that somehow due to these dual objectives, the correct conclusion was broad immunity.); *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 9 (2020).

¹⁴² *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 7, 8, 10 (2020) (citing to *Doe v. Backpage.com, LLC*, 817 F.3d 12, 16-21 (1st Cir. 2016); *M.A. v. Vill. Voice Media Holdings*, 809 F.Supp.2d 1041, 1048 (E.D. Mo. 2011); *Doe v. Bates*, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758, *18 (E.D. Tex., Dec. 27, 2006); even after Justice Thomas’ insights, tech has argued and courts have refused to look more closely at the articulated purposes of Section 230. Instead of self correcting the widely viewed belief the current breadth of the immunity exceeded the intent of Congress, courts have claimed too many companies rely on this broad interpretation and they do not want to upset this reliance; *In re Facebook*, 625 SW.3d 80, 91-93 (Tex. 2021); Daisuke Wakabayashi, *Legal Shield for Social Media Targeted By Lawmakers*, N. Y. TIMES (May 28, 2020), <https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html> (This is a stunning statement given that “the Internet industry has a financial incentive to keep Section 230 intact.”).

misconduct. It simply would give plaintiffs a chance to raise their claims in the first place. Plaintiffs still must prove the merits of their cases, and some claims will undoubtedly fail. Moreover, states and the federal government are free to update their liability laws to make them more appropriate for an Internet-driven society.”¹⁴³

This represents the human toll of this expansion of §230 immunity from its intended narrow scope. It is not simply a failure to adhere to Congressional intent or to the text of the statute. One of the articulated purposes of the CDA and §230 was to shield children from harmful content and harm of CSAM. This broad interpretation not only exposes them to harm, but also precludes them from access to justice. When an ICS facilitates the dissemination of CSAM a victim survivor has no recourse to hold that ICS accountable civilly for their repeated exploitation because the ICS asserts immunity before they can even obtain discovery and have their day in court.

III. Two Decades Later §230 has Failed to Achieve Its Promise Regarding Child Protection

A. The Harm

Recognizing some of the roots of §230 as an amendment to the Communications Decency Act are in child protection, it has been an unabashed failure when it comes to CSAM. As discussed, §230 came out of Conference Committee and was voted on by Congress as a part of the Communications Decency Act and both pieces of legislation promised to offer some protection for children from explicit images – both their exposure to them and the horrifying

¹⁴³ Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 9-10 (2020); For a discussion of how the tech industry actively thwarted enforcement of criminal sex trafficking laws, state development of civil and criminal liability for online sex trafficking, and victim survivor civil suits, see Mary Graw Leary, *History Repeats Itself: The Faces Behind Sex Trafficking are More Familiar Than You Think*, 68 EMORY L. J. ONLINE 1083 (2019).

reality of the abuse and exploitation CSAM creates in its production and distribution. This is true even if one were to look at the promises of those advocating for IFFE. They promised this approach would lead to tech companies developing and distributing filtering and screening products that would prevent or limit the spread of this material.

Either way, it failed. It did so in large part because courts twisted limited immunity into near de facto absolute immunity, incentivizing companies to do nothing regarding protection because they were free to act with impunity.¹⁴⁴ The tragic result has been an unregulated Internet which produces a global facilitator of child sexual abuse in epic proportions not before witnessed in the world.

While the Internet did not create the problem of CSAM, it does provide offenders with unparalleled opportunities to access, possess, and trade child sexual abuse material, often anonymously. It also allows individuals to connect easily with offenders around the world who share similar sexual interests towards children. [This facilitates] relentless sharing of pre-existent CSAM, but can also provide a fertile network for the creation and distribution of new material.¹⁴⁵

This observation is supported when one examines the volume and content of CSAM as it exists today.

Regarding the amount of CSAM, global estimates all reflect a growing volume of CSAM. The National Center for Missing and Exploited Children (NCMEC) houses the CyberTipline in the United States. The CyberTipline collects all reports of suspected child

¹⁴⁴ Many can theorize as to why many courts blindly followed Zeran and continue to do so. These online child exploitation cases are complex. The technological aspects of the law require some expertise often not the forte of trial court judges. Additionally, CSAM cases involve equally as complex matters and is a difficult topic. These combined with an often uneven level of advocacy in trial courts with tech represented by expert counsel in this area with limitless resources and victim survivors by pro bono attorneys could create a toxic combination in which courts rely on the defendants' representations to resolve the case amid the now context that to rule otherwise would put them at odds with other ill informed courts; *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 9-10 (2020); *In re Facebook*, 625 S.W.3d 80 (Tex. 2021); Daisuke Wakabayashi, *Legal Shield for Social Media Targeted By Lawmakers*, N. Y. TIMES (May 28, 2020), <https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html>.

¹⁴⁵ CANADIAN CENTRE FOR CHILD PROTECTION, SURVIVOR'S SURVEY, Executive Summary at 2 (2017).

exploitation online effectively functioning as the “911” of online sexual exploitation of children. In 1998, when the CyberTipline opened it had approximately 4500 reports.¹⁴⁶ The year 2014 marked the first year it received greater than 1 million reports.¹⁴⁷ The following year it recorded 4.4 million reports, which doubled the following year.¹⁴⁸ In 2020, NCMEC reported an unprecedented 21.7 million reports. For 2021, NCMEC received 29.3 million reports and received from law enforcement 85 million images (both still and video) of suspected CSAM, a 35% increase from 2020.¹⁴⁹ Today, NCMEC averages 80,000 reports *per day*. Of the material in 2021, 39.9 million were images and 44.8 million were videos; meaning that in the recent years, video depictions of child sexual exploitation outpace still images of this material.¹⁵⁰

Interpol analyzed the International Database of Child Sexual Exploitation images – a collection of unique images seized by law enforcement throughout the world. This collection is described as a very small proportion of the total volume of images. Yet, in 2018 this database included over 1 million images from 88 countries.¹⁵¹

This volume is not only depicted in dark corners of the Internet, but in mainstream locations as well. “Depictions of child abuse also appear on mainstream sites like Twitter, Reddit and Facebook. And Google supports the business models of companies that thrive on

¹⁴⁶ Statement of Yiota Souras, Sr. Vice President, National Center for Missing and Exploited Children, EARN IT Act Press Conference, February 18, 2022.

¹⁴⁷ Statement of Yiota Souras, Sr. Vice President, National Center for Missing and Exploited Children, EARN IT Act Press Conference, February 18, 2022.

¹⁴⁸ Statement of Yiota Souras, Sr. Vice President, National Center for Missing and Exploited Children, EARN IT Act Press Conference, February 18, 2022.

¹⁴⁹ CyberTipline 2021 Report, National Center for missing and Exploited Children, available at <https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata>.

¹⁵⁰ Statement of Yiota Souras, Sr. Vice President, National Center for Missing and Exploited Children, EARN IT Act Press Conference, February 18, 2022 (These trends are echoed by the Canadian Centre for Child Protection, which in 2017 averaged approximately 4000 tips per month, 98% of them being child sexual abuse imagery.); Canadian Centre for Child Protection, Survivor’s Survey, Executive Summary at 1 (2017).

¹⁵¹ INTERPOL, TOWARDS A GLOBAL INDICATOR ON UN IDENTIFIED VICTIMS OF CHILD SEXUAL EXPLOITATION MATERIAL at 1 (2018).

child molestation. Google returns 920 million videos on a search for ‘young porn.’ Top hits include a video of a naked “very young teen” engaging in sex acts on video along with a video on Pornhub whose title is unprintable ...”¹⁵²

Pornhub is an example of a platform existing on the Internet advertising to be a place where users can upload or download user generated content. A measure of visits puts Pornhub as the tenth most popular website in the world.¹⁵³ A New York Times expose uncovered on Pornhub thousands of images of CSAM – which Pornhub both denied and monetized.¹⁵⁴ The expose noted that at that time an uploader need not verify the age or consent of the subject and Pornhub profits from such images.¹⁵⁵ After this reporting, Visa and MasterCard ceased doing business with Pornhub and it was forced to remove a majority of its 13.5 million videos to offer less than 3 million, suggesting that such a number of videos could not be verified as consensual or not CSAM.¹⁵⁶ Although it previously denied the presence of CSAM on its platform, it then began a practice of requiring verification prior to uploading.¹⁵⁷

¹⁵² Nicolas Kristof, *The Children of Pornhub*, N.Y. TIMES (Dec. 4, 2020), <https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html>.

¹⁵³ *Most Popular Websites Worldwide As Of November 2021*, By Total Visits, <https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/#professional>; Jane Doe #1 v. MG Freesites, Ltd., No. 7:21-cv-00220-LSC, 2022 U.S. Dist. LEXIS 23199 at *3 (N.D. Ala Feb. 9, 2022) (In pending litigation, a district court noted in its denial of motion to dismiss that victims of CSAM allege that in one year 7 million new videos were uploaded, 3.9 billion searches and 24 billion visits occurred – representing similar traffic than Amazon and Netflix.).

¹⁵⁴ Nicolas Kristof, *The Children of Pornhub*, NY TIMES (Dec. 4, 2020), <https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html>.

¹⁵⁵ Nicolas Kristof, *The Children of Pornhub*, NY TIMES (Dec. 4, 2020), <https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html>; Jane Doe #1 v. MG Freesites, Ltd., No. 7:21-cv-00220-LSC, 2022 U.S. Dist. LEXIS 23199 at *3 (N.D. Ala Feb. 9, 2022).

¹⁵⁶ Jordan Valinsky, *Pornhub Removes a majority of its videos after investigation reveals child abuse*, MERCURY NEWS (Dec. 15, 2020), <https://www.mercurynews.com/2020/12/15/pornhub-removes-a-majority-of-its-videos-after-investigation-reveals-child-abuse/>.

¹⁵⁷ Jane Doe #1 v. MG Freesites, Ltd., No. 7:21-cv-00220-LSC, 2022 U.S. Dist. LEXIS 23199 at *3 (N.D. Ala Feb. 9, 2022).

It is not only the volume of CSAM that is of concern, it is the content as well. The Interpol study of its International Child Sexual Exploitation database found a link between the age and severity of images, with the younger the child the more severe the sexual abuse.¹⁵⁸ Great Britain's Internet Watch Foundation's research found a similar result. Specifically, images with children less than 10 years old are the highest in severity and 86% of those images are babies and toddlers.¹⁵⁹ The New York Times reported that Pornhub allowed and monetized videos with violent titles such as "Screaming Teen" and "Degraded Teen."¹⁶⁰ A study of the most actively traded child sexual abuse material found increasing sexual content (defined as penetrating sexual contact between adults and children or sadism and bestiality).¹⁶¹

The age alone of the children depicted in the CSAM available on platforms with immunity demonstrates the failure of §230's goals. 56.2% of Interpol's database depicts prepubescent children.¹⁶² This is consistent with Internet Watch's analysis of its images of which 42% depict children ages 7-10.¹⁶³ Of the survivors interviewed for the Canadian Centre analysis, 56% reported that their abuse began between the ages 0-4 and 87% reported it began when they were 11 years old or younger.¹⁶⁴ Similarly, the expose of Pornhub revealed that a

¹⁵⁸ INTERPOL, TOWARDS A GLOBAL INDICATOR ON UN IDENTIFIED VICTIMS OF CHILD SEXUAL EXPLOITATION MATERIAL at 5 (2018).

¹⁵⁹ INTERPOL, TOWARDS A GLOBAL INDICATOR ON UN IDENTIFIED VICTIMS OF CHILD SEXUAL EXPLOITATION MATERIAL at 5 (2018) (It found 84.2 % of these images were "explicit erotic posing or explicit sexual activity, assault, gross assault, sadism, or other problem paraphernalias.").

¹⁶⁰ Nicolas Kristof, *The Children of Pornhub*, NY TIMES (Dec. 4, 2020), <https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html>.

¹⁶¹ Michael Seto, et al., Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims, National Center for Missing and Exploited Children (March 2018).

¹⁶² INTERPOL, TOWARDS A GLOBAL INDICATOR ON UN IDENTIFIED VICTIMS OF CHILD SEXUAL EXPLOITATION MATERIAL at 5 (2018).

¹⁶³ INTERNET WATCH FOUNDATION, INTERNATIONAL DATA OVERVIEW (2020), available at <https://annualreport2020.iwf.org.uk/trends/international/overview>.

¹⁶⁴ CANADIAN CENTRE FOR CHILD PROTECTION, SURVIVOR'S SURVEY, Executive Summary at 13 (2017).

search on that site for “girls under 18” or “14 year old” connected to more than 100,000 videos.¹⁶⁵

Not only is the immunized Internet the home to such material harmful to children – the very reality that §230 and the CDA were passed to prevent not facilitate – but the harm is felt disproportionately by girls. Interpol found that 64.8% of the unidentified media files depicted female children and offenders are adult men.¹⁶⁶ The largest platforms profit from this exploitation. Mindgeek, the parent company of Pornhub, has been described as the tech company with the third greatest impact on American society, after Facebook and Google.¹⁶⁷

The harm of CSAM is well documented. Because images of child sexual abuse are traded throughout the world in perpetuity a victim survivor suffers lifelong consequences. “Survivors live with the ‘debilitating fear that photos and videos memorializing their sexual abuse as a child and shared on the Internet will forever remain online for anyone to see.’”¹⁶⁸ The recent Canadian Center for Child Protection’s Survivors Survey found that “[r]ecording the sexual abuse of a child has a significant, lifelong impact on the victim. The fact that images/videos of a child’s sexual abuse were created at all, as well as the fact that they may still be possessed by the abuser and be publicly available for others to access, has an enormously negative impact on the individual.”¹⁶⁹ This impact can include trauma, depression, difficulty in romantic/sexual relationships, difficulty in friendship, and physical suffering including “the

¹⁶⁵ Nicolas Kristof, *The Children of Pornhub*, NY TIMES (Dec. 4, 2020), <https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html>.

¹⁶⁶ INTERPOL, TOWARDS A GLOBAL INDICATOR ON UN IDENTIFIED VICTIMS OF CHILD SEXUAL EXPLOITATION MATERIAL at 3 (2018).

¹⁶⁷ *The Tech Companies that have had the biggest Impact on Society in the 21st Century*, DIGGITY MARKETING, <https://diggitymarketing.com/most-influential-tech-companies-2020/> (last visited Apr. 4, 2022).

¹⁶⁸ Captured on Film, SURVIVORS OF CHILD SEX ABUSE MATERIAL ARE STUCK IN A UNIQUE CYCLE OF TRAUMA, National Center for Missing and Exploited Children (2019), available at <https://www.missingkids.org/content/dam/missingkids/pdfs/Captured%20on%20Film.pdf>.

¹⁶⁹ CANADIAN CENTRE FOR CHILD PROTECTION, SURVIVOR’S SURVEY, Executive Summary at 9,28 (2017).

physical pain (e.g., around the genitals), accompanying somatic symptoms (such as headaches, loss of appetite, and sleeplessness), and feelings of psychological distress (emotional isolation, anxiety, and fear).”¹⁷⁰ Young children report feelings of disgust and shame about their self-image entering puberty.¹⁷¹ The Department of Justice discussed the harms of being depicted in CSAM:

When these images are placed on the Internet and disseminated online, the victimization of the children continues in perpetuity. Experts and victims agree that victims depicted in child pornography often suffer a lifetime of re-victimization by knowing the images of their sexual abuse are on the Internet forever. The children exploited in these images must live with the permanency, longevity, and circulation of such a record of their sexual victimization. This often creates lasting psychological damage to the child, including disruptions in sexual development, self-image, and developing trusting relationships with others in the future.¹⁷²

This is echoed by survivors themselves who discussed that CSAM affects them differently than child sexual abuse, pointing to “permanence of the images and the fact if these images are distributed their circulation will never end.”¹⁷³

Indeed, the Supreme Court has recognized the lifelong harms of CSAM when it noted, The full extent of this victim's suffering is hard to grasp. ... These crimes [sexual abuse] were compounded by the distribution of images of her abuser's horrific acts, which meant the wrongs inflicted upon her were in effect repeated; for she knew her humiliation and hurt were and would be renewed into the future as an ever-increasing number of wrongdoers witnessed the crimes committed against her.¹⁷⁴

Survivors not only report fear of being recognized but those who have been recognized report being re-victimized through assaults, stalking, or blackmail.¹⁷⁵ To say this distribution impacts

¹⁷⁰ CANADIAN CENTRE FOR CHILD PROTECTION, SURVIVOR’S SURVEY, Executive Summary at 9, 29 (2017).

¹⁷¹ Captured on Film, SURVIVORS OF CHILD SEX ABUSE MATERIAL ARE STUCK IN A UNIQUE CYCLE OF TRAUMA, National Center for Missing and Exploited Children (2019), available at <https://www.missingkids.org/content/dam/missingkids/pdfs/Captured%20on%20Film.pdf>.

¹⁷² *Child Pornography*, U.S. DEPT. OF JUST., <https://www.justice.gov/criminal-ceos/child-pornography> (last visited Apr. 4, 2022).

¹⁷³ Canadian Centre for Child Protection, Survivor’s Survey, Executive Summary at 28 (2017).

¹⁷⁴ *Paroline v. U.S.*, 572 U.S. 434 (2014).

¹⁷⁵ Canadian Centre for Child Protection, Survivor’s Survey, Executive Summary at 28 (2017).

all aspects of victim survivors' lives is an understatement. Victim survivors report negative impacts on their educational success, maintaining employment, and sleeping difficulties.¹⁷⁶

The harm to CSAM is not *only* to the children *in* the images, but also to the children *exposed* to the images.¹⁷⁷ While there may be an open debate about the harm of pornography, the research is fairly settled that the not yet fully formed adolescent brain can be harmed by such exposure.¹⁷⁸ And youth are indeed exposed to this material. Some researchers suggest that the average age of exposure to pornography is between 11 and 12.¹⁷⁹

The developing adolescent brain lacks the cognitive capability to understand and process the material, particularly if violent.¹⁸⁰ Violent pornography “normalizes sexual harm ... and, in some instances, violence and rape.”¹⁸¹ One study of middle and high school aged youth found that youth exposed to pornography were 6.5 times more likely to be sexually aggressive and another 24 times more likely.¹⁸²

Additionally, survivors of child sexual assault report offenders showing CSAM to them to normalize child sexual assault and desensitize them.¹⁸³ This is precisely a concern of the senators passing the CDA.¹⁸⁴ In addition to that harm, “victims carry the additional trauma that

¹⁷⁶ Canadian Centre for Child Protection, *Survivor's Survey*, Executive Summary at 30, 32 (2017).

¹⁷⁷ For a full discussion of the harm of pornography to children both in and outside the CSAM images see Mary Graw Leary, *Self-Produced Child Pornography: The Appropriate Legal and Societal Response to Juvenile Self Exploitation*, 15 VA. LAW & SOC. POL'Y 1, 9-17 (2008).

¹⁷⁸ Rothman, E.F. *Pornography & Public Health*, Oxford Univ. Press (2021).

¹⁷⁹ Rothman, E.F. *Pornography & Public Health*, Oxford Univ. Press (2021).

¹⁸⁰ Brown, J.A. & Wisco, J.J. The components of the adolescent brain and its unique sensitivity to sexually explicit material, 72 J. OF ADOLESCENCE, 10-13 (2019).

¹⁸¹ Allison Baxter, *How Pornography Harms Children: The Advocate's Role*, ABA (2014).

¹⁸² Allison Baxter, *How Pornography Harms Children: The Advocate's Role*, ABA (2014) (citing Michele Ybarra et al., X-rated material and perpetration of sexually aggressive behavior among children and adolescents: Is There A Link?, 37 AGGRESSIVE BEHAVIOR 1, 3, 7 (2011)).

¹⁸³ Captured on Film: Survivors of CSAM Are Stuck in A Unique Cycle of Trauma, National Center for Missing and Exploited Children, 16 (2019).

¹⁸⁴ See supra notes 22-26.

the imagery of their own abuse is weaponized against other children as a grooming technique.”¹⁸⁵

Twenty-six years after the passage of §230, the fears of the Senate have not only been realized, but surpassed. Not only is explicit content easily available on the Internet, but harmful illegal CSAM is as well. This illegal material is monetized by several of these platforms who do so with impunity.

B. The Law

Given the long history of §230’s intent for limited immunity for Good Samaritans followed by tech defendants and courts transforming that into near *de facto* absolute immunity, courts do not seem to be prepared to restore §230 to its intended purpose. This is true even in CSAM cases which have a history similar to the general §230 cases following Zeran’s broad language.¹⁸⁶ After decades of cases granting motions to dismiss, more recently some courts addressing CSAM and §230 are revisiting this blind adherence to Zeran and allowing some to survive the motion to dismiss stage.¹⁸⁷ However, many more CSAM cases, some even after §230 was amended to exclude sex trafficking cases from §230 immunity, continue to grant motions to dismiss in CSAM cases.¹⁸⁸

¹⁸⁵ See *supra* notes 22-26.

¹⁸⁶ *E.g.*, *Doe v. AOL*, 783 So. 2d 1010, 104 (2001); *Doe v. Bates*, 2006 WL 3813758 (ED Tex. 2006) (Yahoo! Afforded immunity for hosting Candyman child pornography forum).

¹⁸⁷ *E.g.*, *Doe v. MG Freesites*, No. 7:21-cv-00220-LSC (ND AL Feb. 9, 2022); *Does No. 1-50 v. MG Freesites*, Case No. 20-cv-2440-WQH-KSC (S.D. Cal. October 26, 2021).

¹⁸⁸ *E.g.*, *Doe v. Twitter, Inc.*, 21-cv-00485-JCS (N.D. Cal. Aug. 19, 2021) (denying motion to dismiss for TVPA claim, but granting it for the CSAM claim); *LLC v. Touns*, 429 SW.3d 752 (Tex. App. Beaumont 2014) (In a case involving nonconsensual pornography, a Texas appellate court afforded GoDaddy.com with immunity from civil suit, noting that no provision of the CDA limits its application to constitutionally protected speech. GoDaddy.com.).

After the 1991 ruling in favor of AOL, the presence of CSAM has continued to explode online and the harm suffered by its victims was recognized by the Supreme Court.¹⁸⁹ Following the passage of SESTA-FOSTA, some victim survivors sued ICS's for sex trafficking claims, and also included CSAM claims. These cases met mixed results. In *Doe v. MG Freesites*, the District Court Alabama noted that "Congress enacted §230 of the Communications Decency Act to incentivize interactive computer services to protect children, not immunize them for intentionally or recklessly harming them."¹⁹⁰ The Court went on to find it "untenable" to apply §230 immunity to platforms knowingly possessing and distributing CSAM."¹⁹¹ In so doing it specifically referenced prior courts' blind following of *Zeran*, noting that *Zeran* was not a CSAM case, critiquing cases that treat CSAM "the same way as courts have treated speech, such as defamatory statements instead of treating it as illegal contraband."¹⁹² The Central District of California also allowed a case against Pornhub to survive a motion to dismiss.¹⁹³

However, many other cases have not been as thorough with §230's purpose. Recently, a minor boy sued Twitter alleging that it refused to remove the plaintiff's CSAM images even after informing Twitter the age of the victim. Although the court denied the motion to dismiss the trafficking claim due to SESTA, it ruled the CSAM remained within §230 protection and even with the allegation that Twitter monetized the images and knowing allowed them to be distributed, Twitter still was granted immunity.¹⁹⁴ Similarly, the Texas Supreme Court denied

¹⁸⁹ *Paroline v. U.S.*, 572 U.S. 434 (2014).

¹⁹⁰ *Doe v. MG Freesites*, No. 7:21-cv-00220-LSC (ND AL Feb. 9, 2022).

¹⁹¹ *Doe v. MG Freesites*, No. 7:21-cv-00220-LSC (ND AL Feb. 9, 2022).

¹⁹² *Doe v. MG Freesites*, No. 7:21-cv-00220-LSC (ND AL Feb. 9, 2022).

¹⁹³ *Doe v. Twitter, Inc.*, 21-cv-00485-JCS (N.D. Cal. Oct. 26, 2021).

¹⁹⁴ *Doe v. Twitter, Inc.*, 21-cv-00485-JCS (N.D. Cal. Oct. 26, 2021).

Facebook's immunity claim for sex trafficking allegations but granted it for the state common law claims.¹⁹⁵

IV. Potential Path To Bring §230 of the CDA Back to Its Purpose

These statistics reflect the scope with which §230 has been divorced from its original promise as a piece of legislation with child protection as one of its goals. The prior legislative history demonstrates that Congress passed §230 as part of the CDA and a larger package which had as one of its objectives the protection of children. The very Internet that Congress sought to prevent has not only emerged, it has exceeded the fears of Congress.

Not only are these numbers and content stark, but they stand in absolute contrast to the Internet that Congress experienced or even predicted in 1996. The Supreme Court at that time described an Internet so primitive to the modern reader to include terms such as “chat rooms,” “electronic mail,” “mail exploder,” and described a webpage as a place where a “surfer can move a ‘mouse’ and can even communicate with the author of the webpage.”¹⁹⁶ It was in this climate §230 was created, and that Internet has been replaced by a much more rapid and sophisticated one.

Yet, while tech companies are constantly evolving for profit, they have, at best, failed to deploy child protection capabilities to the extent possible.¹⁹⁷ Regarding sexual exploitation

¹⁹⁵ In re Facebook, 625 SW3d 80 (Tex. 2021).

¹⁹⁶ Reno v. A.C.L.U., 521 U.S. 844, 853 (1997).

¹⁹⁷ Dr. Hany Farid, the University of California Berkley professor developed a technology in conjunction with NCMEC and Microsoft in 2008 that can detect CSAM. This product, Photo DNA, has been very effective, yet, he notes how tech companies “drag their feet” in utilizing and improving the technology; Safeguarding Podcast – Digital Crime Scenes : Digital DNA with Professor Hany Farid (Sept. 11, 2021) available at <https://safetonetfoundation.org/2021/09/11/safeguarding-podcast-digital-crime-scenes-digital-dna-with-professor-hany-farid/>.

material, the Court stated in 1996 that “[t]hough such material is widely available, users seldom encounter such content accidentally...Almost all sexually explicit images are preceded by a warning.”¹⁹⁸ As evidenced by the above statistics, that assertion is simply incorrect.

Of particular concern is the Court’s acknowledgment that effective filters do not exist but “will soon be widely available.” This is simply not true today and as an industry, one in possession of de facto absolute immunity, it never utilized their ability to have controls in place.

The modern internet is infested with stomach-churning images of children who have been brutally assaulted and exploited, and who are haunted by a lifetime of pain after these photographs and videos are circulated online. Tech companies have long had ready access to low-cost, or even free tools to combat the scourge of child sexual abuse material but have failed to act.¹⁹⁹

Given this multi-billion-dollar sex industry, no doubt tech companies will not act, as creating or utilizing such accessible and effective products will hurt many tech companies’ bottom lines. “The Internet industry has a financial incentive to keep Section 230 intact. The law has helped build companies worth hundreds of billions of dollars with lucrative business model of placing ads next to largely free content from visitors.”²⁰⁰ The problem is, much of that free content that they monetize is CSAM. While they claim “Congress enacted 230’s broad immunity to remove disincentives for the development and utilization of blocking and filtering technologies...”²⁰¹, such has not occurred. This reality “illustrates the extensive immunity that

¹⁹⁸ Reno v. A.C.L.U., 521 U.S. 844, 855 (1997).

¹⁹⁹ Press Release, Graham, Blumenthal Introduce EARN IT Act to Encourage Tech Industry to Take Online Child Sexual Exploitation Seriously (January 31, 2022) (statement of Senator Richard Blumenthal), available at <https://www.lgraham.senate.gov/public/index.cfm/2022/1/graham-blumenthal-introduce-earn-it-act-to-encourage-tech-industry-to-take-online-child-sexual-exploitation-seriously>.

²⁰⁰ Daisuke Wakabayashi, *Legal Shield for Social Media Targeted By Lawmakers*, N.Y. TIMES (May 28, 2020), <https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html>.

²⁰¹ Doe v. America Online, 783 So.2d 1010, 1015 (2001) (quoting Zeran, 129 F.3d at 331).

the current formulation of the CDA already extends to social media companies' activities undreamt of in 1996. It therefore may be time of to reconsider the scope of 230.”²⁰²

One of the reasons this *de facto* near absolute immunity has occurred is because the tech industry and its surrogates have sought to reframe §230 as stand-alone legislation that guaranteed not just the limited liability it the text, but a form of *de facto* absolute immunity unimaginable in 1996.²⁰³ The effects of this overstated immunity are many, allowing immunity claims for product defects, terrorism, sex trafficking, and other allegations Congress never intended to include in the limited Good Samaritan or non-publisher immunity. In the area of CSAM legislation has been proposed which offers a path out of the ocean of CSAM that resides on Internet platforms with impunity. The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2021 (EARN IT Act) is designed to address some of the CSAM problems §230 has helped create. This bipartisan legislation was proposed by a Republican Senator with 21 co-sponsors: 11 Republicans and 10 Democrats.²⁰⁴ Its title derives from the notion that ISP’s seem to have this broad immunity, never intended by Congress, and have done little to address the concerns of Congress. One of those concerns is CSAM. With regard to that issue, the proposed legislation seems to suggest immunity for CSAM violations is inappropriate.

Many have made suggestions on how to address some of these issues. These include repeal of §230, ending engagement based business model which encourages harmful content,

²⁰² Michael D. Smith and Marshall Van Alstyne, It’s time to Update Section 230, HARVARD BUS. REV. (August 12, 2021).

²⁰³ For a discussion of tech company’s efforts to thwart any measure to limit immunity *see* Mary Graw Leary, *History Repeats Itself: The Faces Behind Sex Trafficking are More Familiar Than You Think*, 68 EMORY L. J. ONLINE 1083 (2019).

²⁰⁴ EARN IT Act, S. 3538, 117th Cong. (2022).

algorithmic changes, issue based amendments.²⁰⁵ Even Mark Zuckerberg publicly claims support for some version of regulation.²⁰⁶ The EARN It Act consists of four main components, three of which are most relevant to this article. It officially changes the label of “child pornography” to CSAM throughout the federal code.²⁰⁷ It also amends §230(e) to include CSAM offenses among those that have been excluded from this immunity. Currently, §230 excludes from immunity federal criminal statutes, certain intellectual property, certain communications privacy law, certain state laws “not inconsistent with” §230, and most recently, sex trafficking laws.²⁰⁸ This Act would add certain child sexual exploitation laws, including civil claims brought by victim survivors pursuant to their rights of a private right of action in 18 U.S.C. 2255, as well as certain state criminal and civil laws claims related to CSAM.²⁰⁹

As this bill and others were debated tech companies and their surrogates have claimed they may be unable to take the necessary steps to eliminate or deter CSAM from their sites.²¹⁰ Given the immense ability many tech companies have to collect data from users, analyze and monetize that information, it is hard to imagine they cannot take steps to limit this material. Even if they were to struggle with such an obligation, The EARN IT Act created a National Commission on Online Child Sexual Exploitation Prevention to “develop recommended best

²⁰⁵ Margaret Reardon, *Section 230: How It Shields Facebook and Why Congress Wants Changes*, CNET NEWS (Oct. 6, 2021); Oscar Gonzales, *Bill Unveiled to Reduce Section 230 Protections for Social Media Companies*, CNET TECH (Feb.5, 2021).

²⁰⁶ Margaret Reardon, *Section 230: How It Shields Facebook and Why Congress Wants Changes*, CNET NEWS (Oct. 6, 2021); Oscar Gonzales, *Bill Unveiled to Reduce Section 230 Protections for Social Media Companies*, CNET TECH (Feb.5, 2021) (Indeed, in 2019, the Business Roundtable announced that corporate goals should extend beyond shareholder value.); David Gelles and David Yaffe-Bellany, *Shareholder Value is no Longer Everything*, N.Y. TIMES (Aug.19, 2019), <https://www.nytimes.com/2019/08/19/business/business-roundtable-ceos-corporations.html>.

²⁰⁷ S.3536, 117th Cong. § 6 (2022); S.3536, 117th Cong. §§ 7, 8 (2022) (It also makes several technical amendments to modernize the CyberTipline and reporting requirements.).

²⁰⁸ 47 U.S.C. § 230(e).

²⁰⁹ S.3536, 117th Cong. § 5 (2022).

²¹⁰ Joseph Marks, *Most Cyber Pros Give Thumbs Down to the EARN IT Act*, WASH. POST (Feb. 23, 2022) (quoting Senator Richard Blumenthal describing “Big tech and their army of lobbyists and allies.”).

practices that providers of computer services may choose to implement to prevent, reduce, and respond to online sexual exploitation of children.’²¹¹ This Commission is designed to receive the input from various stakeholders about best practices from diverse perspectives. While some members include law enforcement or victim survivors, these perspectives also include members nominated by both the majority and minority of the Congress in fields such as civil liberties, privacy, computer science, or software engineering.²¹² Membership also includes 4 individuals who currently work for ICS’s and represent “diverse types of businesses and areas of professional expertise,” some of which are from companies with over 30 million monthly users and others of which have less than 10 million monthly users.²¹³

This legislation is narrow in scope, addressing only one of the myriad of problems presented by §230: CSAM.²¹⁴ It also has no penalty for the failure of a company to follow the best practices. It does nothing to address the problem of the Internet’s lack of regulation. Many have called for a wholesale update of §230. This approach continues a piecemeal approach to a medium arguably more fundamental than many utilities.

While perhaps only incremental, it does return §230 to its original framing of a legislative effort to protect children in a dawning Internet. At that time, Congress did not know what the Internet would become. It now does know what it has become regarding CSAM and must act.

²¹¹ S.3536, 117th Cong. § 3(b) (2022); C.F., *US v. Walther*, 652 F.2d 788 (9th Cir. 1981) (This provision notes the voluntary nature of complying with the best practices. If an ICS prefers another method to prevent CSAM dissemination is free to adopt that method. Therefore, following these best practices provide optional guidance and avoids the state actor doctrine); *US v. Privdahl*, No. CR 13-18-H-DLC (D. Mont. March 6, 2014).

²¹² S.3536, 117th Cong. § 3(c) (2022).

²¹³ S.3536, 117th Cong. § 3(c) (2022).

²¹⁴ S.3536, 117th Cong. 7(a)(2022) (Tech has criticized the bill as an effort to preclude end to end encryption. However, Senator Leahy added an amendment to the bill which explicitly states that the use of encryption shall not “serve as an independent basis for liability of a provider of an interactive computer service for a claim or charge.”); *see also* comments of Senator Graham, U.S. Committee on Judiciary 1:48:50 (“legislation is not about encryption or free speech); Comments of Richard Blumenthal (calling this critique a “gigantic red herring propagated by Big tech and their armies of lobbyists and their allies).

Conclusion

The purpose of the Telecommunications Act of 1996 was to update the 1934 Communications Act.²¹⁵ Part of that update was to update the child protection laws to respond to the new potential problems of the Internet. Section 230 and the CDA were part of that solution. The promise of the CDA has not been realized and §230 no longer – if it ever did – achieves its goals. Legislation restoring §230 to its original purpose is needed and the EARN It Act is one path to take to restore balance at least between the legal regime involving CSAM and the Internet.

²¹⁵ S. Rep. No. 104-230 (1996) (comments of Senator Pressler).